

PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

Claims 1-11 (Canceled)

12. (Currently Amended) A method for fast generation of a cryptographic key, comprising:
generating a first public key for encrypting a first wireless communication; and
generating, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the [[a]] second wireless communication, wherein the second public key is independent of the first public key; ~~and~~
~~determining whether the second public key has been stored prior to establishing the second wireless communication.~~

13. (Canceled)

14. (Currently Amended) The method of claim 32 [13], further comprising:
using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

15. (Currently Amended) The method of claim 32 [13], further comprising:
generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

16. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:
means for generating a first public key for encrypting a first wireless communication; and
means for generating, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the [[a]] second

wireless communication, wherein the second public key is independent of the first public key;
and

~~means for determining whether the second public key has been stored prior to
establishing the second wireless communication.~~

17. (Canceled)

18. (Currently Amended) The wireless communication device of claim 33 [17], further comprising:

means for using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

19. (Currently Amended) The wireless communication device of claim 33 [17], further comprising:

means for generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

20. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for generating a first public key to encrypt a first wireless communication and generating, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the [[a]] second wireless communication; and

a memory for storing the second public key,
wherein the second public key is independent of the first public key ~~and further~~
~~wherein the processor determines whether the second public key has been stored prior to~~
~~establishing the second wireless communication.~~

21. (Currently Amended) A processor for fast generation of a cryptographic key, said processor being configured to:

generate a first public key for encrypting a first wireless communication; and
generate, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the [[a]] second wireless communication, wherein the second public key is independent of the first public key; ~~and~~
~~determine whether the second public key has been stored prior to establishing the second wireless communication.~~

22. (Currently Amended) A computer program product comprising instructions for fast generation of a cryptographic key, wherein the instructions upon execution cause a computer to:
generate a first public key for encrypting a first wireless communication; and
generate, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in the [[a]] second wireless communication, wherein the second public key is independent of the first public key; ~~and~~
~~determine whether the second public key has been stored prior to establishing the second wireless communication.~~

23. (New) The computer program product of claim 22, wherein the instructions upon execution further cause a computer to:
determine whether the second public key has been stored prior to establishing the second wireless communication.

24. (New) The computer program product of claim 23, wherein the instructions upon execution further cause a computer to:
use the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

25. (New) The computer program product of claim 23, wherein the instructions upon execution further cause a computer to:
generate a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

26. (New) The processor of claim 21, wherein said processor is further configured to:
determine whether the second public key has been stored prior to establishing the second
wireless communication.

27. (New) The processor of claim 26, wherein said processor is further configured to:
use the second public key to encrypt the second wireless communication when it is
determined that the second public key has been stored.

28. (New) The processor of claim 26, wherein said processor is further configured to:
generate a third public key to encrypt the second wireless communication when it is
determined that the second public key has not been stored.

29. (New) The wireless communication device of claim 20, wherein the processor
determines whether the second public key has been stored prior to establishing the second
wireless communication.

30. (New) The wireless communication device of claim 29, wherein the processor uses
the second public key to encrypt the second wireless communication when it is determined that
the second public key has been stored.

31. (New) The wireless communication device of claim 29, wherein the processor
generates a third public key to encrypt the second wireless communication when it is determined
that the second public key has not been stored.

32. (New) The method of claim 12, further comprising:
determining whether the second public key has been stored prior to establishing the
second wireless communication.

33. (New) The wireless communication device of claim 16, further comprising:

means for determining whether the second public key has been stored prior to establishing the second wireless communication.